

Cyber Security Awareness as Critical Driver to National Security

Joey Jansen van Vuuren, Cyber Defense Research Group, Council for Scientific and Industrial Research, Pretoria, South Africa

Marthie Grobler, Cyber Defense Research Group, Council for Scientific and Industrial Research, Pretoria, South Africa

Jannie Zaaïman, University of Venda, Thohoyandou, South Africa

ABSTRACT

In South Africa, cybersecurity has been identified as a critical component contributing to National Security. More rural communities are becoming integrated into the global village due to increased hardware and software corporate donations, the proliferation of mobile Internet devices and government programmes aimed at bridging the digital divide through major broadband expansion projects. The authors' research shows that many of the new Internet users are not aptly trained to protect themselves against online threats, leaving them vulnerable to online exploits and inherently exposing the national system to potential international cyber attacks. This article works toward the identification of any correlation between the economic development and mobile use propensity of Internet users with regard to National Security. Internet penetration statistics are used in correlation with the economic development and exposure to technological advances of South Africans to classify participants in the surveys used into three groups: urban netizens, semi-rural netizens and rural netizens. South African citizens from areas within the Gauteng, Limpopo and Mpumalanga provinces participated in this study. Separate from these criteria, the availability of and access to the Internet via mobile phones is also taken into consideration. The article uses the results from the surveys to identify direct and indirect links between the factors in question.

Keywords: Awareness, Cyber Security, National Security, Rural Communities, South Africa

INTRODUCTION

With the proliferation of technology and networked devices through all scopes of life, cybersecurity awareness is becoming a more prominent driver in the positioning of National

Security within a country. This article investigates the influence of cybersecurity awareness levels as driver towards National Security, based on a South African case study. The research is investigative in nature and aims to identify any connections between the level of cyberse-

DOI: 10.4018/ijcwt.2012010103

curity awareness of different citizen groups as impacting the level of National Security within that group.

In South Africa, cybersecurity has been identified as a critical component, as noted by Palesa Legose, Director of Cybersecurity at the South African Department of Communications: *“The government views cyber crime in a serious light, and therefore aims to launch an awareness programme and establish a National Cybersecurity Advisory Council (NCAC) in collaboration with the private sector, to step up the fight against cyber crime”* (BiztechAfrica, 2012b). The importance of cybersecurity with regard to National Security is corroborated by Stella T Ndabeni, South African Communications Deputy Minister: *“The Internet has also attracted illicit activities, commonly referred to as cyber crimes, which, in some cases, cannot only be detrimental to individuals, but [are] also capable of causing massive disruptions of economies of nations”* (Moyo & Kayle, 2012).

Especially in Africa, rural communities are becoming integrated into the global village at a fast pace. This is in part due to increased hardware and software corporate donations from global organisations, but is also supported by the proliferation of web enabled mobile devices and government programmes aimed at bridging the digital divide through major broadband expansion projects. Comprehensive research conducted by the authors show that many of the new Internet users are not aptly trained to protect themselves against online threats, leaving them vulnerable to online exploits and inherently exposing the national system to potential international cyber attacks. This research will form the foundation of this study with the premise that cybersecurity awareness is an active driver towards National Security.

Background to the Study

The increase in African broadband access has had a significant effect on the Internet access of South Africa. With more South Africans connected to the Internet, and a large portion of this population that has either not had ad-

equate training in cybersecurity awareness, or regular and sustained exposure to technology and broadband Internet access, South Africa is currently much more exposed to cyber threats than before the significant increase in broadband availability in 2009 (Grobler, Jansen van Vuuren, & Zaaïman, 2011). As an additional threat, South Africa is in many ways the Internet entry point to the African continent and could therefore be used as a central point for launching cyber warfare type attacks on the rest of the world (Jansen van Vuuren, Phahlamohlaka, & Brazzoli, 2010). In this context, it is important that cybersecurity awareness in the broader South Africa communities is addressed appropriately to prevent South Africans from falling victim to cyber criminals. An increase in cybersecurity awareness will also prevent South African citizens from inadvertently being used as digital soldiers in cyber attacks against other countries. In normal combat, soldiers are part of armies controlled by defence forces to perform attacks. In contrast, digital soldiers use cyber space to perform attacks (Dunnigan, 1996), not necessarily controlled by military commanders. In these attacks, regular citizens can be used as digital soldiers to spread malware or do denial of service attacks, without their knowledge.

According to 2007/2008 statistics, only 4% of the continental population in Africa was estimated to have Internet access. The Internet access in Africa has increased to 27% of the total Internet access in the world by 2011 (Rosewarne, 2012).

The African continent, as shown in Figure 1, is estimated to have an Internet penetration of 15.6% by June 2012 (Internet World Stats, 2012). This indicates a significant rise in Internet access for South African citizens since 2007. In 2012, South Africa is estimated to have an Internet penetration of just below 20%, with the number of Internet users increasing from 6.8 million in 2010 to 8.5 million by December 2011 (Speckman, 2012). As such, the development of the African undersea cables was a much needed addition to Africa's technological readiness. Most of the undersea cables featured in Figure 2 have already been activated (Song, 2012).

10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/cyber-security-awareness-critical-driver/75763

Related Content

Provably Secure Private Set Intersection With Constant Communication Complexity

Sumit Kumar Debnath (2019). *International Journal of Cyber Warfare and Terrorism* (pp. 39-64).

www.irma-international.org/article/provably-secure-private-set-intersection-with-constant-communication-complexity/231643

IP-CHOCK Reference Detection and Prevention of Denial of Service (DoS) Attacks in Vehicular Ad-Hoc Network: Detection and Prevention of Denial of Service (DoS) Attacks in Vehicular Ad-Hoc Network

Karan Verma (2021). *Research Anthology on Combating Denial-of-Service Attacks* (pp. 579-601).

www.irma-international.org/chapter/ip-chock-reference-detection-and-prevention-of-denial-of-service-dos-attacks-in-vehicular-ad-hoc-network/262001

On Experience of Social Networks Exploration for Comparative Analysis of Narratives of Foreign Members of Armed Groups: IS and L/DPR in Syria and Ukraine in 2015-2016

Yuriy V. Kostyuchenko, Maxim Yuschenko and Igor Artemenko (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 1656-1671).

www.irma-international.org/chapter/on-experience-of-social-networks-exploration-for-comparative-analysis-of-narratives-of-foreign-members-of-armed-groups/251516

Violencia de Estado, guerra, resistencia. Por una nueva política de la Izquierda

Maximiliano E. Korstanje (2011). *International Journal of Cyber Warfare and Terrorism* (pp. 53-55).

www.irma-international.org/article/violencia-estado-guerra-resistencia-por/74154

A Vulnerability-Based Model of Cyber Weapons and its Implications for Cyber Conflict

Christian Czosseck and Karlis Podins (2012). *International Journal of Cyber Warfare and Terrorism* (pp. 14-26).

www.irma-international.org/article/vulnerability-based-model-cyber-weapons/75762